Santé Ontario

Normes de service provinciales sur les portails de patients (PP)

Juin 2021

TABLE DES MATIÈRES

Reconnaissance

Les exigences énumérées dans ce document s'inspirent d'autres normes provinciales, notamment de la *norme de vérification des visites virtuelles* et de la *norme relative à la réservation de rendez-vous en ligne*, et elles ont été passées en revue par les dirigeants régionaux et les experts internes.

Nous tenons à remercier les personnes et les organisations suivantes pour leurs importantes contributions à ce document.

Dale Anderson – Services de technologie de l'information numérique sur la santé à Hamilton Health Sciences
John Haywood – Services de technologie de l'information numérique sur la santé à Hamilton Health Sciences
Devi Pandya– Services de technologie de l'information numérique sur la santé à Hamilton Health Sciences
Mark Berry – Services de technologie de l'information numérique sur la santé à Hamilton Health Sciences
Marzena Cran – Services de technologie de l'information numérique sur la santé à Hamilton Health Sciences
Josh Sinclair – Services de technologie de l'information numérique sur la santé à Hamilton Health Sciences

Conseillers des patients
Santé Ontario
Ministère de la Santé
Fournisseurs de portails de patients

Avis de non-responsabilité

Le présent document concerne les services provinciaux de Santé Ontario ou d'autres organismes provinciaux de santé, mais ne leur est pas spécifique. La norme décrite dans ce document est une norme non normalisée et, par conséquent, des erreurs, des omissions et des révisions peuvent survenir. Le présent document n'est pas destiné à être un avis juridique et ne doit pas être considéré comme en étant un. Santé Ontario encourage la consultation d'un conseiller juridique au besoin.

Vous voulez recevoir ces informations dans un format accessible?
1-877-280-8538, ATS 1-800-855-0511 info@ontariohealth.ca.

1. Introduction

Les technologies numériques dans le domaine de la santé offrent de plus en plus aux équipes de soins la possibilité de déployer des outils de technologies de l'information et des outils de communication auprès des patients. Ceux-ci permettent aux patients, aux aidants et aux professionnels de la santé d'accéder plus efficacement aux données et aux informations, améliorant ainsi la qualité des résultats en matière de santé. Les portails de patients peuvent servir de plateforme efficace pour soutenir les interactions entre les patients et leurs équipes de soins de santé et pour accéder aux dossiers médicaux et aux ressources d'éducation en santé de manière sûre et sécurisée. La présente norme a pour but de faciliter la sélection et la mise en œuvre de solutions numériques de portails de patients.

Les objectifs de ces normes sont les suivants :

- Définir les exigences fonctionnelles et non fonctionnelles générales des solutions numériques utilisées par les organismes de santé et les cliniciens pour prendre en charge des plateformes de portail patient (PPP) qui partagent numériquement des informations cliniques avec les utilisateurs (patients).
- Définir un cadre et des exigences obligatoires que la plateforme doit démontrer concernant la diffusion numérique d'informations cliniques aux utilisateurs.
- Aider les fournisseurs de services de santé à choisir des solutions conçues pour favoriser la sécurité et la confidentialité des données cliniques auprès des utilisateurs et faire progresser l'échange interopérable de renseignements sur la santé.
- Guider les organismes de soins de santé, y compris les équipes Santé Ontario, qui souhaitent se procurer une solution de PPP.
- Fournir aux équipes Santé Ontario les recommandations et les facteurs à considérer nécessaires pour maximiser la valeur de leur investissement dans l'acquisition d'une première PPP ou la mise à niveau d'une PPP existante.

Les lecteurs doivent reconnaître que les normes ne tentent pas de définir les exigences pour chaque fonction de la plateforme et qu'elles ne recommandent aucune PPP en particulier.

1.1 Principes directeurs

Les organismes qui décident de diffuser des informations cliniques aux utilisateurs sous forme numérique doivent suivre les principes fondamentaux clés des soins de santé, en plus de la Déclaration de valeurs des patients pour l'Ontario[1] :

1. Le patient est propriétaire de ses renseignements personnels sur la santé (RPS), lesquels doivent être conçus dans un format convivial et portable.
2. Le patient a le droit d'accéder pleinement à ses RPS à tout moment par l'intermédiaire du bureau de diffusion de l'information des établissements sources.
3. Tous les efforts doivent être déployés pour permettre aux patients d'accéder aux RPS avec peu ou pas de restrictions; à défaut de quoi une voie claire d'accès en temps réel doit être mise en place.
4. Le patient a le droit d'être informé et de contrôler qui a accès aux RPS pertinents qui sont partagés.
5. Le patient a le droit de s'assurer de l'exactitude et de l'exhaustivité de ses RPS.

2. Glossaire

Les définitions fournies dans cette section proviennent de diverses sources et sont présentées dans le but de fournir des descriptions non techniques et simplifiées de certains des termes utilisés dans ce document.

Plateforme de portail de patients (PPP)
Les plateformes de portail de patients (PPP) sont des applications de services de santé numériques conçues pour automatiser la prise de contact avec les patients et maintenir l'engagement de ces derniers tout au long du continuum de soins. Les PPP courantes comprennent les portails de patients, les applications mobiles pour les plateformes Android/iOS et les agents conversationnels avec messagerie. Les PPP peuvent donner aux patients le sentiment d'être connectés et pris en charge, et améliorer leur expérience et leur satisfaction.[2]

Prise de rendez-vous en ligne
Les solutions de prise de rendez-vous en ligne permettent aux patients de réserver un rendez-vous en personne, par vidéo ou par téléphone, en choisissant une date et une heure et en recevant une confirmation de rendez-vous automatisée, avec peu ou pas d'interaction avec une autre personne. Les rappels de rendez-vous sont automatisés, soit par courriel, message texte ou enregistrement vocal.[3]
Les adresses courriel et les formulaires de demande de renseignements en ligne ne sont pas des solutions de prise de rendez-vous en ligne, car ils nécessitent une interaction humaine pour confirmer la disponibilité des rendez-vous.

Consultations virtuelles
Une consultation virtuelle est une interaction numérique au cours de laquelle un ou plusieurs cliniciens, notamment des médecins, des infirmières ou des professionnels paramédicaux, fournissent des services de soins de santé à un patient ou à son aidant.

Services de santé numériques
Les services de santé numérique décrivent les nombreuses utilisations des technologies de l'information qui soutiennent la prestation de soins aux patients dans le système de santé. Cela peut inclure l'utilisation coordonnée du Web, des technologies mobiles et infonuagiques pour intégrer les points de soins.[4]

Littératie en santé
La littératie en santé est le degré auquel un individu a la capacité d'obtenir, de communiquer, de traiter et de comprendre des informations et des services de santé de base afin de prendre des décisions appropriées en matière de santé.[5]

Interopérabilité
L'interopérabilité est la capacité de saisir, de gérer, de communiquer et d'échanger des données de manière précise, efficace, sûre et cohérente avec différents systèmes de technologies de l'information, applications logicielles et réseaux dans divers contextes, et d'échanger des données de sorte que l'utilisation de l'objectif clinique ou opérationnel et la signification des données restent inchangés.[6]

Portail de patient
Les portails de patients sont des innovations technologiques qui permettent aux patients d'accéder électroniquement à leurs RPS.[7]

Mesures des résultats déclarés par les patients (MRDP)
Les MRDP sont des instruments de mesure (c'est-à-dire des enquêtes) que les patients remplissent pour fournir des informations sur des aspects de leur état de santé et de leur qualité de vie, notamment leurs symptômes, leur fonction, leur niveau de douleur et leur santé physique et mentale. Les cotes Oxford Hips et Knees Scores sont des exemples de MRDP qui pourraient être transmises aux patients dans un portail de patients.[8]

Mesures des expériences déclarées par les patients (MEDP)
Les MEDP sont des instruments de mesure (c'est-à-dire des enquêtes) que les patients remplissent pour fournir des informations sur leur point de vue concernant le niveau de soins qu'ils ont reçu.[9]

Obligatoire (O)
Obligatoire (O) fait référence à une exigence qui doit être satisfaite.[10]

Recommandé (R)
Recommandé (R) fait référence à une exigence facultative.[10]

Futur (F)
Une exigence qui est prévue pour l'avenir.

3. Accès numérique des patients à leurs dossiers médicaux

3.1 Exigences fonctionnelles

Toutes les solutions d'engagement des patients doivent respecter un ensemble d'exigences fonctionnelles de base, en plus des exigences fonctionnelles propres à la solution (c'est-à-dire les portails de patients, la prise de rendez-vous, etc.). Voici les exigences fonctionnelles communes à prendre en compte pour toutes les solutions :

- Sécurité – cryptage, connexion sécurisée, etc.
- Mise à jour – directives de publication des données, réduction des délais au minimum.
- Exhaustivité – limiter les sections à accès restreint – montrer autant que possible toutes les informations du dossier du patient.
- Portable – permet l'utilisation hors ligne, le partage avec d'autres professionnels de la santé à l'extérieur de la province ou du pays.
- Téléchargeable – l'utilisateur peut suivre et mettre à jour ses dossiers de santé personnels (données sur la condition physique, etc.).
- Partageable – délégation – et possibilité de partager avec les aidants (téléchargement vers d'autres dossiers de santé électroniques – voir aussi la section « Portable »).
- Possibilité de restriction – l'utilisateur peut restreindre les données partagées avec les aidants et les délégués.
- Auditable – l'utilisation de l'application doit pouvoir être examinée.

En plus de la conformité générale à la LAPHO, la liste suivante de fonctionnalités communes doit être utilisée lors de la création ou de l'acquisition d'un logiciel de portail de patients qui sera destiné au public.
Les sections suivantes contiennent des tableaux d'exigences qui utilisent les en-têtes de colonne suivants :

- # – identifiant unique de l'exigence
- Exigence – une déclaration décrivant un besoin que les solutions de portail de patients devront satisfaire.
- Priorité – indique l'importance de l'exigence, avec « O » = obligatoire ou « R » = recommandé.
- Notes – informations ou conseils supplémentaires pour aider à interpréter l'exigence.

Fonctionnalité générale

#	Exigence	Priorité	Notes
3.1.1	La plateforme permet aux utilisateurs de s'inscrire ou de se connecter à des comptes.	O	L'inscription est liée au profil de l'utilisateur.
3.1.2	La plateforme doit permettre de fournir et de modifier ou de supprimer l'accès aux délégués et aux mandataires.	O	La plateforme permet un accès autorisé aux aidants inscrits.[11]
3.1.3	La plateforme doit être capable de récupérer des données provenant de différentes sources en utilisant un critère de correspondance commun.	O	Exemples : numéro de carte de santé, numéro de dossier médical, date de naissance.
3.1.4	La plateforme doit garantir que tous les utilisateurs existants de la plateforme peuvent également consulter leurs RPS à partir de leur profil dans le portail de patients existant (en cas de mise en œuvre ou de mise à niveau d'une solution existante).	O	L'accès à la plateforme ne doit pas être affecté par les changements et les mises à jour du système.
3.1.5	La plateforme doit permettre à un utilisateur de visualiser les tests de laboratoire et l'imagerie diagnostique.	O	Les attentes concernant le calendrier de disponibilité des résultats sur la plateforme doivent être fournies. Une interprétation de la terminologie médicale doit être donnée.
3.1.6	La plateforme doit permettre à l'utilisateur de voir ses rendez-vous passés et futurs.	O	Liste des rendez-vous passés et futurs.

#	Exigence	Priorité	Notes
3.1.7	Donner aux utilisateurs la possibilité d'imprimer ou de sauvegarder une copie hors ligne des aspects concernant leurs RPS.	O	Dossiers médicaux et résumés cliniques contenant des informations pertinentes et exploitables sur les soins de santé de l'utilisateur[1].
3.1.8	Permet à l'utilisateur de recevoir, de remplir et de renvoyer au prestataire de services des formulaires ou des questionnaires d'inscription remplis.	O	Les formulaires envoyés à l'utilisateur doivent être modifiables et l'utilisateur doit avoir la possibilité de les soumettre.
3.1.9	La plateforme doit permettre l'utilisation d'autres critères de comparaison des patients lorsqu'un numéro de carte de santé n'est pas disponible.	R	Les sources suivantes font référence à des groupes de patients dénués d'assurance-maladie qui n'ont pas accès à un numéro de carte santé : L'Assurance-santé de l'Ontario pour tous (en anglais seulement) Débats sur les enjeux de santé (en anglais seulement)
3.1.10	La plateforme doit permettre à l'utilisateur d'avoir accès à son prestataire au moyen de consultations virtuelles.	R	Veuillez consulter les exigences concernant les consultations virtuelles. https://otn.ca/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf

#	Exigence	Priorité	Notes
3.1.11	La plateforme doit permettre d'utiliser et d'afficher les exigences terminologiques acceptées telles que SNOMED, LOINC, pCLOCD, etc.	R	L'objectif n'est pas que le portail des patients traduise ou transcrive les informations provenant des sources, mais plutôt qu'il soit en mesure d'exploiter les informations supplémentaires disponibles grâce à ces normes terminologiques. Voici des exemples d'exigences terminologiques : • SNOMED CT (Systematized Nomenclature of Medicine – Clinical Terms) – Exigences internationales en matière de terminologie contrôlée des termes cliniques. • LOINC (Logical Observation Identifiers Names and Codes) – Exigences internationales en matière de terminologie contrôlée pour les laboratoires et les documents. • pCLOCD (Base de données pancanadienne des codes d'observation de laboratoire) – Exigences en matière de terminologie contrôlée pour les laboratoires canadiens. • Ensembles de valeurs HL7 FHIR – Ensembles de valeurs définis pour être utilisés avec HL7 FHIR; comprennent les exigences en matière de terminologie contrôlée. • Sous-ensembles terminologiques pancanadiens – Ensembles terminologiques d'Inforoute Santé du Canada publiés en fonction des besoins canadiens; comprennent des exigences de terminologie contrôlée fondées sur les exigences terminologiques internationales • ICD-10-CA (Classification statistique internationale des maladies et des problèmes de santé connexes, 10e révision – Amélioration canadienne) – Nécessite une licence de l'Institut canadien d'information sur la santé; système international de classification des maladies cliniques avec extensions canadiennes. • CCI (Classification canadienne des interventions en santé) – Nécessite une licence de l'Institut canadien d'information sur la santé; système international de classification des interventions cliniques avec extensions canadiennes.

#	Exigence	Priorité	Notes
3.1.12	La plateforme doit prévoir une notification pour signaler la récupération d'informations nouvelles ou modifiées.	R	Des notifications poussées opportunes, pertinentes pour l'utilisateur, reflétant les niveaux de priorité et pouvant être archivées.
3.1.13	Permettre l'utilisation de la plateforme comme lieu central pour saisir/agréger leurs RPS provenant de sources externes.[2]	R	Diverses options de saisie de données, y compris en texte libre, et la possibilité de synchroniser avec d'autres sources de données, y compris des applications tierces, comme Fitbit, les carnets de vaccination, les applications de santé et de conditionnement physique, les dispositifs médicaux.
3.1.14	Permettre à l'utilisateur de dialoguer avec ses fournisseurs au moyen d'un système de messagerie sécurisé.[3]	R	Système de communication bidirectionnel avec cryptage de bout en bout ou possibilité d'intégration avec une solution tierce. Pour plus de détails, veuillez vous référer à la norme relative aux consultations virtuelles, qui contient les exigences provinciales en matière de messagerie sécurisée pour la prise de rendez-vous en ligne. https://otn.ca/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf
3.1.15	Permettre à l'utilisateur de demander l'accès ou le transfert de dossiers et de résumés de santé entre prestataires de services.	R	Les fournisseurs de services actuels ou précédents de l'utilisateur qui utilisent la même plateforme ou se connectent à d'autres plateformes.
3.1.16	Permet à l'utilisateur de s'engager dans des activités de gestion des médicaments et de demander le renouvellement des ordonnances.	R	Liste des médicaments, dosages avec des instructions claires (sans abréviations); possibilité d'envoyer une demande de renouvellement d'ordonnance; ou capacité à s'intégrer à une solution tierce.

Audit et sécurité

#	Exigence	Priorité	Notes
3.1.17	La plateforme doit être capable de produire des journaux d'audit sur l'activité des comptes utilisateurs.	O	Liste des connexions précédentes affichant la date, l'heure et le type d'appareil.

#	Exigence	Priorité	Notes
3.1.18	Permettre aux utilisateurs de se déconnecter de leur profil en ligne.	O	Messages contextuels pour confirmer la sélection de l'option de déconnexion, puis de la déconnexion réussie par l'utilisateur.
3.1.19	Permettre aux utilisateurs de visualiser et d'effectuer des audits de l'activité de leur propre compte.	R	Il est recommandé aux organismes d'autoriser les utilisateurs à effectuer un auto-audit.

Conception et interface utilisateur

#	Exigence	Priorité	Notes
3.1.20	Garantir que la plateforme et les données affichées sont accessibles depuis un ordinateur de bureau (Mac/PC/Linux) et des plateformes mobiles (Android/iOS).	O	La plateforme doit être conçue pour être compatible avec les systèmes d'exploitation existants.
3.1.21	S'assurer que la plateforme affiche les renseignements sur la santé de l'utilisateur dans un format organisé, p. ex., le diagnostic, le plan de traitement, les résultats de laboratoire, etc.	O	Les informations sont disponibles sous forme de sous-rubriques.
3.1.22	Permettre aux utilisateurs de communiquer avec leur fournisseur de services en ayant la possibilité de demander, de recevoir et/ou de télécharger des documents.	O	Les formats privilégiés pour les fichiers sont ceux qui sont largement acceptés et spécifiés en tant que fichiers PDF, DOC et JPEG.
3.1.23	Possibilité pour la plateforme d'inclure une solide fonctionnalité d'aide aux utilisateurs.	O	Exemples : Incorporer des descriptions appropriées ou des conseils pour aider les utilisateurs ayant une littératie limitée en matière de santé à trouver et à comprendre les regroupements de données dans la plateforme. Incorporer l'utilisation d'aides visuelles (icônes ou images) pour aider les utilisateurs à mieux comprendre les types de regroupements de renseignements sur la santé.

#	Exigence	Priorité	Notes
3.1.24	Permettre une interface en anglais et en français pour les utilisateurs.	R	Les équipes Santé Ontario doivent s'assurer qu'elles répondent aux besoins en services de santé en français de leur communauté locale, y compris les exigences législatives, le cas échéant.
3.1.25	Capacité de la plateforme à afficher les données dans un format convivial.	R	L'organisation des informations agrégées peut ne pas être facile, mais elle est nécessaire pour offrir aux utilisateurs un moyen unique et direct d'accéder à leurs données médicales, dans le souci d'une expérience utilisateur optimale. Une étude de Vreeman et Richoz (2015) suggère que « la pléthore de conventions idiosyncrasiques pour identifier le même contenu clinique dans différents systèmes d'information constitue un obstacle fondamental à la pleine exploitation du potentiel des DES ».[11]
3.1.26	Permettre une interface patient multilingue.	R	Prendre en charge les langues autres que l'anglais et le français.

Administration

#	Exigence	Priorité	Notes
3.1.27	Donner aux équipes Santé Ontario et aux organismes fournisseurs la possibilité de préciser le contenu de certaines parties de la plateforme afin de permettre des communications personnalisées et une diffusion ciblée.	O	Le contenu et le moment de l'envoi des informations doivent être pertinents pour répondre aux besoins de l'utilisateur en ce qui a trait à ses renseignements sur la santé.
3.1.28	Possibilité pour la solution de bloquer ou de retarder des dossiers cliniques précis.	O	Dans certains cas, l'organisme estime que l'information doit être restreinte ou retardée pour des raisons cliniques ou de sécurité.
3.1.29	Mettre à la disposition des utilisateurs un espace qui leur donnera des détails sur la plateforme et ce qu'elle peut leur apporter.	R	Une vidéo de présentation pour éclairer l'utilisateur sur la façon de naviguer, expliquer les principales caractéristiques et les avantages potentiels.

#	Exigence	Priorité	Notes
3.1.30	S'assurer que la plateforme dispose d'une section consacrée au matériel d'information.	R	Afin de tenir les utilisateurs informés de la manière d'utiliser la plateforme et des différentes options de l'application. Mettre périodiquement à jour le manuel de l'utilisateur, en indiquant la date de la dernière révision.
3.1.31	Donner aux utilisateurs la possibilité de demander la mise à jour du dossier médical.	R	Sans objet
3.1.32	Donner aux utilisateurs la possibilité d'effectuer des paiements de factures en ligne.	R	Sans objet

Intégrations

Indépendamment de la capacité d'une plateforme à afficher les données provenant des différents répertoires et sources de données, les organismes doivent s'assurer que les accords de partage de données adéquats sont en place avec les dépositaires de l'information sur la santé.

#	Exigence	Priorité	Notes
3.1.33	Permettre à la plateforme d'adhérer aux exigences communes d'interopérabilité, comme DHIEX.	O	Ontario. (2020, 20 avril). Politique d'échange de renseignements numériques sur la santé (en anglais seulement).
3.1.34	Capacité de la plateforme à prendre en charge l'intégration commune de la technologie de consultations virtuelles et à s'aligner sur les nouvelles normes en la matière.	O	https://otn.ca/wp-content/uploads/2020/03/virtual-visits-solution-standard1-1-1-1.pdf
3.1.35	Permettre à la plateforme d'adhérer à des exigences communes en matière de conformité, de validation et de mise en œuvre.	O	Sans objet.

#	Exigence	Priorité	Notes
3.1.36	Permettre à la plateforme d'afficher les données du Système d'information de laboratoire de l'Ontario (SILO).	R	Le SILO est un répertoire unique provincial qui permet d'échanger, par voie électronique et en toute sécurité, toutes les informations relatives aux demandes de tests de laboratoire en Ontario et aux résultats entre les praticiens et les fournisseurs de services de laboratoire autorisés. L'intégration au répertoire du SILO est possible avec la spécification OLIS HL7 FHIR. Spécification d'affichage du SILO : Veuillez consulter le guide de la nomenclature SILO pour connaître la série de normes définies par SILO concernant l'affichage de ses informations.
3.1.37	Capacité de la plateforme à afficher les données des DSE pour les soins primaires.	R	À l'heure actuelle, il n'existe pas d'interface FHIR commune pour les consommateurs. Les organismes qui cherchent à s'intégrer aux DSE devront s'assurer que les accords appropriés sont en place en tant que dépositaires de l'information sur la santé afin de partager ces données avec leurs clients.[12]

#	Exigence	Priorité	Notes
3.1.38	Possibilité pour la plateforme d'afficher des données provenant de divers systèmes d'information sur la santé en matière de soins aigus.	R	Comme il n'existe pas d'application commune du système d'information sur la santé en Ontario, les intégrations avec des instances spécifiques du système d'information hospitalier nécessiteront une collaboration étroite avec les fournisseurs (soins aigus en général) et leurs fournisseurs, au cas par cas, tant sur le plan technique qu'en ce qui concerne les accords. **Systèmes d'information hospitaliers clés en Ontario :** **Cerner** Ressources FHIR : FAQ de Cerner (en anglais seulement) Documentation : Cerner Millennium **EPIC** Ressources FHIR : Epic FHIR **Meditech** Ressources FHIR : API pour les données de santé des patients (en anglais seulement)
3.1.39	La plateforme doit inclure des données provenant d'au moins trois secteurs de la santé.	R	Des exemples de sources de données pourraient notamment inclure : - DSE - Systèmes d'information hospitaliers - Autres systèmes cliniques - Répertoires et sources de données provinciaux - Laboratoires privés et prestataires de services de diagnostic
3.1.40	Possibilité pour la plateforme de se connecter au SMART App Launch Framework afin de connecter des applications tierces et de les lancer de manière autonome ou à partir d'un portail.	R	Le SMART App Launch Framework connecte des applications tierces aux données du dossier médical électronique, ce qui permet de lancer des applications à partir de l'intérieur ou de l'extérieur de l'interface utilisateur d'un système de DSE. Cadre SMART pour le lancement d'une application (en anglais seulement)

#	Exigence	Priorité	Notes
3.1.41	Capacité pour la plateforme d'afficher les données d'un des visualiseurs provinciaux.	F	Bien qu'il soit possible de se connecter directement à des hôpitaux individuels (des ressources sont fournies ci-dessous à cet effet), il est conseillé aux organismes de s'intégrer plus facilement et plus efficacement à l'un des visualiseurs provinciaux (ClinicalConnect ou Connecting Ontario), car les aspects techniques de l'intégration avec plusieurs hôpitaux ont déjà été mis au point. Les organismes pourraient ainsi se concentrer sur l'obtention d'accords de partage de données avec les différents hôpitaux pour y accéder. Actuellement, ClinicalConnect a une API destinée aux consommateurs disponible et implémentée. **Visualiseurs provinciaux :** **ClinicalConnect** À propos de ClinicalConnect ClinicalConnect (cyberSanté Ontario) **Connecting Ontario** Visualiseur clinique de ConnexionOntario
3.1.42	Possibilité pour la plateforme d'afficher les données du Répertoire numérique des immunisations (RNI).	F	Le RNI est le répertoire actuel des immunisations pour la province de l'Ontario. Il contient des informations sur l'immunisation en matière de santé publique et plus de 90 millions de dossiers de vaccination standardisés pour plus de 6 millions de clients, avec plus de 2 000 utilisateurs inscrits.
3.1.43	Possibilité pour la plateforme d'afficher des données provenant du répertoire des données cliniques sur les soins actifs et communautaires.	F	Le répertoire des données cliniques sur les soins actifs et communautaires permet d'accéder aux renseignements sur les patients qui proviennent des hôpitaux et des organismes de services de soins à domicile et en milieu communautaire de partout en Ontario.

#	Exigence	Priorité	Notes
3.1.44	Capacité pour la plateforme d'afficher les données du Répertoire numérique des médicaments (RNM).	F	Le Répertoire numérique des médicaments (RNM) est un répertoire électronique d'informations sur les médicaments dispensés et les services pharmaceutiques. Le RNM comprend actuellement des dossiers relatifs aux médicaments financés par les deniers publics et les services de pharmacie, ainsi que toutes les drogues contrôlées, ce qui représente environ 70 % du total des médicaments dispensés en Ontario.
3.1.45	Capacité pour la plateforme d'afficher des données provenant du répertoire d'imagerie diagnostique (Diagnostic Imaging- Common Services DI-CS).	F	Les répertoires d'imagerie diagnostique contiennent les rapports d'imagerie diagnostique des clients des services de santé et les images numériques, comme les radiographies, l'imagerie par résonance magnétique (IRM) et les échographies. On retrouve quatre répertoires d'imagerie diagnostique en Ontario (connus sous le nom de DI-Rs), chacun desservant une région géographique différente de la province.

Identité, accès et autorisation

#	Exigence	Priorité	Notes
3.1.47	La plateforme doit prendre en charge l'authentification des utilisateurs conformément aux normes provinciales (par exemple, la politique de l'ICA) avant de diffuser les RPS.	O	Authentification multicouche pour vérifier l'identité du patient. La plateforme doit au moins permettre aux utilisateurs d'être identifiés par leur numéro de carte Santé, leur date de naissance et leur nom de famille.

#	Exigence	Priorité	Notes
3.1.48	Capacité de la plateforme à prendre en charge l'identité numérique, l'authentification et l'autorisation du patient.	O	Santé Ontario en est cours d'acquisition d'une solution de portefeuille numérique et de pièces d'identité vérifiables en appui à plusieurs applications et API destinées aux patients de l'Ontario. Les objectifs de cette solution sont les suivants : Fournir un accès simple, pour l'utilisateur et le fournisseur (aspiration future), aux services de santé de Santé Ontario (et du secteur des soins de santé en général) au moyen d'un ensemble d'API publiées ou d'applications. Réduire au minimum la nécessité de partager ou de produire les mêmes renseignements personnels à plusieurs reprises avec chacun des services de soins de santé qu'un utilisateur souhaite utiliser. Ne partager que la quantité de renseignements personnels nécessaires au service en question et à l'identification de la personne concernée. Réduire au minimum les différents identifiants et mots de passe que les utilisateurs doivent utiliser et éliminer la nécessité des mots de passe en général. Simplifier le processus d'identification et d'inscription aux services et rendre l'authentification aux différents services fluide et aussi transparente que possible. Comme cette solution n'est pas encore disponible, les implantations actuelles de solutions orientées vers les patients bénéficieraient de l'utilisation de cette solution ou de cette approche.
3.1.49	La plateforme doit pouvoir mettre en œuvre une forme d'authentification à facteurs multiples (AFM) pour les utilisateurs qui se connectent au site.	R	Il est fortement recommandé que les connexions des utilisateurs soient au moins aussi rigoureuses que celles des institutions financières, sinon plus.

Inscription

#	Exigence	Priorité	Notes
3.1.50	Offrir aux utilisateurs un moyen simple et convivial de s'inscrire.	O	Par exemple : Les utilisateurs devront avoir une adresse courriel valide et la saisir lors de leur inscription à la plateforme, en plus des informations d'identification (p. ex., nom et prénom, numéro de carte Santé).
3.1.51	Un courriel d'inscription standard sera envoyé à l'adresse courriel que l'utilisateur a fournie lors de son inscription.	O	Sans objet

3.2 Exigences non fonctionnelles

En plus des exigences fonctionnelles, des exigences non fonctionnelles supplémentaires doivent être prises en compte pour tous les logiciels.

#	Description	Priorité	Notes
3.2.1	**Performance** Capacité de l'interface utilisateur à fonctionner de manière optimale selon les spécifications de l'industrie.	O	Exemple : Temps de réponse de l'application pour accomplir les tâches suivantes : a) chargement initial de l'écran, maximum de 3 secondes; b) 80 % des écrans ne doivent pas dépasser une latence dans le temps de réponse de plus de 3 secondes.
3.2.2	**Capacité** Capacité de la plateforme à prendre en charge, en tout temps, un nombre approprié de sessions d'utilisateurs simultanées.	O	Selon la taille de la base d'utilisateurs prévue.
3.2.3	**Disponibilité** Possibilité pour la plateforme d'être toujours disponible, 24 heures sur 24, 365 jours par an.	O	Cette disponibilité exclut les interruptions de service programmées.
3.2.4	**Extensibilité** Capacité de la plateforme à être extensible pour supporter l'augmentation du nombre d'utilisateurs inscrits tout en répondant aux exigences de performance.	O	Sans objet

#	Description	Priorité	Notes
3.2.5	**Facilité d'utilisation** La plateforme doit être conviviale, avec des instructions rédigées dans un langage simple et clair et des menus faciles à utiliser pour faciliter l'exécution des tâches.	O	Sans objet
3.2.6	**Accessibilité** Capacité de la plateforme à être accessible à l'utilisateur dans des formats conformes aux exigences de la LAPHO.	O	Se référer au site Web de la LAPHO pour plus de détails.
3.2.7	**Confidentialité** Capacité de la plateforme à afficher des informations conformes à la LPRPS. Préserver la confidentialité des informations relayées conformément à la politique.	O	Sans objet
3.2.8	**Sécurité** Procéder à l'identification des utilisateurs à l'aide d'un numéro de carte Santé et d'un identifiant/mot de passe unique. Mettre en œuvre des mesures de protection des données pour éviter les brèches de sécurité informatique et renforcer les mesures en la matière.	O	Sans objet
3.2.9	**Interopérabilité** Capacité de la plateforme à être interopérable avec les répertoires provinciaux.	O	Sans objet
3.2.10	**Portabilité** Capacité de la plateforme à être utilisée sur différents systèmes d'exploitation, navigateurs et appareils sans que les performances n'en soient modifiées.	O	Sans objet

#	Description	Priorité	Notes
3.2.11	**Production de rapport** Capacité de la plateforme à indiquer le nombre d'utilisateurs qui sont inscrits à l'application et qui l'utilisent, ainsi que son niveau d'utilisation.	O	Voir ci-dessous : Manuel d'instructions sur les orientations stratégiques Santé Ontario (Services numériques) Doit se conformer à la Politique de rendement et de production de rapports dans le contexte des solutions numériques pour la santé

3.3 Consultations virtuelles

Pour plus d'informations, veuillez vous référer aux Exigences concernant la solution de consultations virtuelles.

3.4 Prise de rendez-vous en ligne

Pour plus d'informations, veuillez vous référer aux Normes sur la prise de rendez-vous en ligne.

4. Exigences relatives à l'interface utilisateur

4.1 Gestion du contenu informationnel

La gestion du contenu informationnel désigne le processus de collecte, de livraison, d'extraction, de gestion et d'administration de l'information. Aux fins du présent document, la gestion du contenu informationnel est étudiée dans le contexte de la collecte, de la fourniture, de l'extraction, de la gestion et de l'administration des renseignements sur la santé par les consommateurs de soins de santé. La section du présent document consacrée à la gestion du contenu informationnel décrit les exigences en matière de données pour les PPP, les exigences relatives à l'état de préparation pour la contribution des données, les lignes directrices pour la diffusion des données, les considérations cliniques et un guide pour l'organisation de l'information au sein d'une PPP. Cela appuie la *Politique d'échange de renseignements numériques sur la santé numérique* (en anglais seulement) qui stipule qu'il est nécessaire de combler les lacunes pour permettre un accès transparent aux dossiers intégrés des patients afin de réduire la fragmentation, les redondances et les incohérentes au chapitre de l'expérience utilisateur.[4] En ce qui concerne les PPP (outre les exigences législatives décrites dans la LPRPS), du point de vue du contenu informationnel, il n'existe pas de normes établies concernant les ensembles de données minimaux qui devraient être mis à disposition sous forme numérique dans les canaux d'accès des patients. Plusieurs facteurs doivent être pris en compte avant qu'un organisme décide de diffuser numériquement des RPS. En essence, ce document préconise que les utilisateurs puissent accéder facilement à toutes leurs données médicales.

4.2 Exigences minimales en matière de données

La plateforme doit être capable d'afficher les données énumérées dans le tableau ci-dessous, tel qu'il est tiré du guide de l'ensemble de données minimal de l'IPS. Veuillez vous référer à la composition de l'IPS pour en savoir plus.

#	Exigence	Priorité	Notes
4.2.1	Sommaire des médicaments	R	Donne l'historique des médicaments actuels et antérieurs.
4.2.2	Allergies	R	Donne une liste des allergies documentées connues.
4.2.3	Liste des problèmes	R	Donne une liste des conditions documentées actuelles.
4.2.4	Immunisation	R	Fournit un historique des immunisations.
4.2.5	Historique des procédures	R	Fournit un historique des consultations et des procédures suivies.
4.2.6	Appareils médicaux	R	Donne une liste des appareils médicaux utilisés par l'utilisateur, par exemple une pompe à insuline, voies centrales, etc.
4.2.7	Résultats des diagnostics	R	Doit inclure toutes les formes de résultats de tests diagnostiques, p. ex., résultats de tests de laboratoire, de radiologie, de cardiologie.
4.2.8	Notes cliniques	R	Indique les notes des interactions cliniques.
4.2.9	Signes vitaux	R	Un historique des signes vitaux enregistrés, p. ex., la tension artérielle, la taille, le poids, l'IMC.
4.2.10	Antécédents de maladie	R	Détails et résumé des antécédents de maladies.
4.2.11	Grossesse	R	Détails sur les grossesses actuelles ou passées.
4.2.12	Historique social	R	Informations sociales, économiques et culturelles.
4.2.13	État fonctionnel	R	Les résultats actuels et historiques de toute évaluation de l'état fonctionnel, p. ex., les MRDP, les détails des soins à domicile et en milieu communautaire concernant les activités de la vie quotidienne.

#	Exigence	Priorité	Notes
4.2.14	Plan de soins	R	Donne tous les plans de soins élaborés, actuels et historiques. Les informations doivent être dynamiques pour refléter les changements en temps réel.
4.2.15	Directives avancées	R	Fournit des détails sur toutes les directives actuelles et précédentes, y compris tout code d'état.[13]
4.2.16	Rendez-vous	R	Référence à la prise de rendez-vous en ligne et aux rendez-vous à l'hôpital.
4.2.17	Recommandations électroniques	R	Fournit des informations actuelles et historiques sur les recommandations électroniques.
4.2.18	Matériel et ressources pédagogiques	R	Matériel et ressources pédagogiques pour l'utilisation de la solution et des renseignements sur la santé.

5. Exigences techniques

5.1 Loi provinciale sur la protection des renseignements sur la santé (LPRPS)

Référez-vous à la Loi de 2004 sur la protection des renseignements personnels sur la santé, L.O. 2004, chap. 3, annexe A

5.2 Exigences en matière de confidentialité et de sécurité

Confidentialité

Les PPP impliquent la collecte, l'utilisation et la divulgation de RPS et de renseignements personnels (RP). Par conséquent, les organismes et les utilisateurs cliniques des PPP doivent s'assurer que leurs activités sont conformes à la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, à la *Loi sur l'accès à l'information et la protection de la vie privée* et aux autres lois pertinentes. D'autres lois peuvent s'appliquer, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* pour l'échange de renseignements personnels et la *Loi canadienne anti-pourriel* (LCAP) pour la messagerie et l'envoi de courriels sécurisés.[14] La transmission électronique d'informations cliniques sur la santé peut présenter certains risques dont il faut tenir compte. Les organismes et les équipes qui utilisent des PPP doivent prévoir les situations qui suivent.

PORTAIL DE PATIENT

- Les informations cliniques d'un patient tombent entre les mains du mauvais patient.
- Partage d'informations cliniques avec le mauvais patient.
- Changement de garde entraînant un accès non autorisé aux RPS d'un patient pédiatrique.
- Message sécurisé envoyé au mauvais patient.

- Divulgation involontaire d'informations sensibles susceptibles de causer un préjudice si elles étaient vues par le patient.

Les organismes et les utilisateurs cliniques peuvent atténuer bon nombre de ces risques en mettant en œuvre des politiques, des procédures et des pratiques appropriées en matière de confidentialité et de sécurité. Certains risques peuvent également être atténués en choisissant des solutions de prise de rendez-vous en ligne et des plateformes de portail de patient qui répondent à un ensemble minimum d'exigences en matière de confidentialité et de sécurité. Pour ce faire, il convient notamment de prendre des mesures raisonnables pour confirmer que les technologies utilisées par les utilisateurs de la plateforme permettent de partager les RPS de manière privée et sécurisée.[15]

Sécurité de l'information

Les organismes de soins de santé et les utilisateurs cliniques doivent s'assurer que leurs fournisseurs de solutions fourniront des services de sécurité de l'information dans le cadre de leurs obligations de service. Par exemple, les solutions doivent comporter des mesures de protection de la sécurité des informations, comme l'accès aux informations, la réponse aux incidents de sécurité, le cryptage, la journalisation et la surveillance, les procédures opérationnelles ainsi que d'autres mécanismes.

Les fournisseurs de solutions décriront et s'engageront formellement à fournir des garanties de sécurité des informations aux organismes de soins de santé et aux utilisateurs cliniques qui mettent en œuvre leurs solutions.

Les exigences suivantes sont guidées par des considérations de confidentialité :

#	Exigence	Priorité	Notes
5.2.1	Publier un avis sur ses pratiques d'information relatives à son PPP et à ses services.	O	Au minimum, l'avis doit décrire la manière dont le fournisseur traite et protège les renseignements personnels et les renseignements sur la santé, ainsi que les droits à la vie privée des utilisateurs.
5.2.2	Désigner un employé responsable de la protection de la vie privée.	O	Les coordonnées du responsable désigné de la protection de la vie privée doivent être accessibles au public sur le site Web du fournisseur.
5.2.3	Disposer d'un programme de confidentialité et de sécurité comprenant des politiques et des procédures.	O	Au minimum, les fournisseurs doivent disposer d'une politique de protection de la vie privée décrivant les règles régissant la collecte, l'utilisation, la divulgation, la conservation, l'exactitude, la sécurité et la disposition des RPS/RP, la gestion des violations, la sécurité des informations, la continuité des activités et la reprise après sinistre, l'accès, la correction et les

#	Exigence	Priorité	Notes
			pratiques en matière de plaintes.
5.2.4	Fournir une piste d'audit électronique de tous les événements, y compris un journal de tous les accès et transferts de RPS.	O	Les registres d'audit doivent enregistrer et conserver les informations relatives aux transactions (c'est-à-dire l'ID de l'événement, la date et l'heure de début et de fin). Les solutions qui conservent des enregistrements récapitulatifs des événements doivent maintenir un journal d'audit qui comprend : • Le type d'informations consultées, manipulées, modifiées ou traitées d'une autre manière; • La date et l'heure auxquelles elles ont été consultées, manipulées, modifiées ou traitées d'une autre manière; • L'identité de toutes les personnes qui ont consulté, manipulé, modifié ou traité les RPS; et • L'identité de la personne à laquelle les RPS se rapportent. Les données du journal d'audit ne doivent pas être modifiées, supprimées ou effacées, mais seulement marquées comme ayant été modifiées, supprimées ou effacées.
5.2.5	Fournir une piste d'audit électronique de l'accès à la piste de solution.	O	La piste d'audit comprendra toutes les tentatives de connexion, qu'elles aient réussies ou échouées. Elle doit enregistrer le trafic qui indique une activité non autorisée sur le serveur de l'application. Le journal doit inclure : • L'estampille temporelle, l'ID utilisateur/identification de l'application, l'adresse IP d'origine, le port accédé ou le nom de l'ordinateur. • Les connexions externes en interface ODBC utilisées pour exécuter des

#	Exigence	Priorité	Notes
			requêtes SQL ou de couche de données. • Les données de l'application stockées à l'extérieur de la base de données, comme les pièces jointes. • Tous les fichiers de données utilisés pour répondre à d'autres exigences locales (par exemple, les exigences en matière de rapports). • L'heure du système doit être synchronisée avec une source fiable pour maintenir l'intégrité de la piste d'audit. • Protection pour garantir l'intégrité de l'audit et contre tout accès, modification et destruction non autorisés.
5.2.6	Mettre en œuvre des garanties et des contrôles raisonnables pour protéger toutes les données, les terminaux et le trafic, qu'ils soient de passage ou inactifs.	O	Les solutions doivent utiliser des mécanismes de cryptage et de hachage conformes aux normes actuelles de l'industrie pour crypter et protéger les RPS et/ou les renseignements personnels. Voici certaines des normes cryptographiques recommandées : NIST SP 800-22 Révision 1a - Une suite de tests statistiques pour les nombres aléatoires et pseudo-aléatoires, FIPS 140-2 - Exigences de sécurité pour les modules cryptographiques.
5.2.7	Fournir un résumé à jour de l'évaluation de l'évaluation des facteurs relatifs à la vie privée (EFVP).	O	Les assurances et les exigences relatives à l'EFVP doivent inclure : • L'EFVP doit avoir été réalisée au cours des deux dernières années avant de chercher à participer au programme de vérification. • L'EFVP doit avoir été réalisée par un professionnel certifié possédant l'un des titres suivants obtenu par l'intermédiaire de l'International Association of Privacy Professionals (IAPP) : Professionnel agréé de l'information et de la protection de la vie privée (CIPP/C); gestionnaire agréé de l'information et de la protection de la vie privée (CIPM); technologue agréé de l'information et de la protection de la vie privée (CIPT) ou détenir au moins deux ans d'expérience dans la réalisation d'évaluations des facteurs relatifs à la vie

#	Exigence	Priorité	Notes
			privée en Ontario et/ou au Canada. • La méthodologie de l'EFVP doit comprendre une analyse législative pertinente à l'Ontario et à son contexte de soins de santé, une description des flux de données et, au minimum, une correspondance complète avec les dix principes d'équité dans le traitement de l'information publiés par le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation (CSA) et avec les lignes directrices sur l'EFVP publiées par la Commission à l'information et à la protection de la vie privée de l'Ontario[11] concernant les soins de santé. • L'EFVP et le résumé de l'EFVP doivent comprendre une table des matières, un résumé des conclusions sur les risques, y compris un tableau de probabilité et d'impact ou une carte des risques, un plan d'atténuation et un état des risques en suspens, ainsi que le nom et les coordonnées de la ou des personnes et/ou de l'organisme qui ont réalisé l'EFVP. Tout risque identifié comme étant élevé doit être atténué avant de faire appel à un fournisseur. Les risques évalués comme étant moyens doivent faire l'objet d'un plan d'atténuation clair avec des délais de clôture dans les six mois suivant l'identification du risque. Une mise à jour des risques moyens doit être effectuée une fois que les activités d'atténuation ont été déployées. • L'EFVP et le plan d'atténuation des risques doivent être approuvés par le représentant autorisé de l'organisme ou le chef de la protection des renseignements personnels du fournisseur de la solution, et un résumé doit être communiqué à Santé Ontario aux fins d'examen. • Les EFVP doivent être mises à jour tous les trois ans ou plus tôt en cas de modification de la solution, de la

#	Exigence	Priorité	Notes
			législation, de la politique ou des activités commerciales du ou des fournisseurs de la solution, par exemple, en cas de changement à la façon dont les renseignements sont recueillis, utilisés ou divulgués, qui pourrait avoir une incidence sur la confidentialité des renseignements sur la santé ou sur le droit à la vie privée.
5.2.8	Fournir une évaluation des menaces et des risques (EMR) à jour au niveau des applications.	O	Les assurances et les exigences relatives à l'EMR doivent inclure : • L'EMR doit avoir été réalisée au cours des deux dernières années et être pertinente pour la solution de PPP soumise à ce processus, sans que des changements importants aient été apportés à la solution, aux services ou au programme de sécurité depuis la réalisation de l'EMR. • Confirmation que l'EMR a été effectuée par un évaluateur qualifié détenant au moins cinq ans d'expérience directe à temps plein dans le domaine de la sécurité, et possédant une certification CISSP en règle. • L'EMR doit avoir été complétée par une analyse de sécurité basée sur une méthodologie d'évaluation des menaces et des risques conforme aux normes de l'industrie (p. ex., HTRA, NIST, OCTAVE). • L'EMR et le résumé doivent inclure un résumé des tableaux de risques et un état des risques. Tous les risques jugés très élevés ou élevés doivent être atténués avant de faire appel à un fournisseur. Les risques moyens doivent faire l'objet de plans d'atténuation clairs et être clos dans les six mois après avoir été relevés. Il est recommandé que les risques faibles soient relevés, surveillés et fermés lorsque cela est possible, et que les résumés soient partagés avec Santé Ontario aux fins d'examen. • L'EMR doit être mise à jour tous les trois ans ou plus tôt en cas de modification de la solution, de la législation, de la politique ou des

#	Exigence	Priorité	Notes
			activités commerciales du ou des fournisseurs de la solution, par exemple en cas de changement à la façon dont les renseignements sont recueillis, utilisés ou divulgués, qui pourrait avoir un impact sur la confidentialité et/ou la sécurité des renseignements sur la santé ou sur le droit à la vie privée. L'EMR doit inclure les résultats d'une analyse de vulnérabilité et d'un test d'intrusion.
5.2.9	Effectuer des analyses périodiques d'évaluation des vulnérabilités.	O	Les analyses de vulnérabilité doivent être effectuées, au minimum, sur une base trimestrielle ou lors de la diffusion d'une version majeure du logiciel ou d'un changement d'architecture ou d'infrastructure majeur. Ces analyses doivent inclure l'application et l'infrastructure de l'application. Pour les environnements hébergés, le fournisseur d'hébergement peut être amené à soumettre ses propres résultats d'analyse des vulnérabilités. Les derniers résultats des analyses de vulnérabilité doivent être soumis avec l'EMR. La preuve que des analyses trimestrielles ont été effectuées peut être demandée dans le cadre du cycle de rafraîchissement triennal de l'EMR.
5.2.10	Effectuer des tests d'intrusion périodiques.	O	Les tests d'intrusion doivent être effectués, au minimum, sur une base annuelle ou lorsqu'il y a eu une version majeure du logiciel, ou un changement d'architecture ou d'infrastructure majeur. Les tests d'intrusion doivent inclure l'application et l'infrastructure de l'application lorsque cela est possible. Pour les environnements hébergés, le fournisseur d'hébergement peut être amené à soumettre les résultats de ses tests d'intrusion. Les derniers résultats des tests d'intrusion doivent être soumis avec l'EMR. La preuve que les tests annuels ont été effectués peut être demandée

#	Exigence	Priorité	Notes
			dans le cadre du cycle de rafraîchissement triennal de l'EMR.
5.2.11	Respecter les contrôles de sécurité et de confidentialité.	O	Les fournisseurs de solutions doivent suivre les orientations générales de sécurité basées sur les objectifs de contrôle de la norme ISO 27002. Veuillez vous référer à la boîte à outils de Santé Ontario sur la sécurité et aux exigences d'hébergement d'OntarioMD pour connaître les exigences liées à la sécurité des applications, à l'infrastructure, aux opérations commerciales et à la continuité des activités. D'autres certifications de sécurité telles que SOC2, Hitrust, OntarioMD, Inforoute Santé du Canada peuvent aider à satisfaire à cette exigence. **Objectifs du contrôle :** • Réseau et opérations • Sécurité physique • Utilisation acceptable de l'information et information **Technologie** •Accès au contrôle et gestion des identités pour l'accès au niveau du système • Gestion des actifs informationnels • Gestion des incidents de sécurité de l'information • Gestion des risques liés aux menaces • Continuité des activités • Cryptographie • Journalisation et surveillance de la sécurité • Fournisseur de services électroniques
5.2.12	Fournir un vaste cadre entourant l'entente pour la solution de PPP et les services connexes, y compris pour toute tierce partie mandatée pour aider à fournir ces services.	O	Les ententes relatives à la solution et aux fournisseurs tiers comprendront, au minimum, des dispositions relatives à la confidentialité et à la sécurité décrivant les services et les mesures de protection administratives, techniques et physiques pour assurer la confidentialité et la sécurité des RPS et des RP, ainsi que la manière dont le fournisseur et tout fournisseur tiers retenu se conformeront aux lois applicables, y compris, mais sans s'y limiter, aux lois énumérées ci-dessus.

#	Exigence	Priorité	Notes
5.2.13	En appui aux obligations et politiques de conservation des organismes de soins de santé ou des cliniciens.	O	Les solutions facilitent ou permettent la collecte et la conservation des RP et des RPS. La solution doit conserver les RP et les RPS conformément aux obligations et aux politiques de tenue de dossiers et de conservation. La solution doit conserver les données conformément aux lois ou normes applicables. En l'absence d'une politique de conservation existante, il est recommandé aux cliniciens de suivre les normes réglementaires et/ou professionnelles applicables, telles que les directives de l'Ordre des médecins et chirurgiens de l'Ontario sur la conservation et la destruction des données dans le cadre de la politique de gestion des dossiers médicaux.
5.2.14	S'assurer que le fournisseur de solutions stocke tous les RPS sur des systèmes situés au Canada.	O	Le stockage des RPS sur des serveurs hébergés dans un centre de données canadien (y compris les sauvegardes) augmentera probablement la confiance et le confort des utilisateurs et leur volonté d'utiliser la plateforme.
5.2.15	Demander aux utilisateurs de consentir à ce que les RPS soient stockés en dehors de leur province de résidence.	O	Les utilisateurs seront informés que le système peut stocker des RPS à l'extérieur de leur province de résidence et qu'ils doivent consentir à ce stockage. Cela peut se faire au moyen de « conditions d'utilisation » ou d'un « contrat d'utilisation », rédigé en langage clair, qui doit être accepté lors du processus de création du compte utilisateur.

Annexe A : Recommandations concernant la mise en place progressive des normes de compatibilité

Bien que le présent document ne puisse pas prescrire la méthodologie à suivre pour la mise en place progressive des normes de compatibilité, il formule les recommandations suivantes :

1. Déterminer clairement les lacunes actuelles en matière de compatibilité.
   Détailler et délimiter clairement les zones ou les éléments qui ne répondent pas aux critères précis.
2. Mesurer l'effort à fournir pour combler les lacunes.
   Déterminer le coût global en ce qui a trait aux efforts, au temps et aux ressources pour combler les lacunes en matière de compatibilité. Notez que dans les cas où des solutions existantes sont en place, le coût de la correction peut être plus élevé que celui de la recherche d'une nouvelle solution.
3. Consulter toutes les parties prenantes.
   Déterminer les priorités en recueillant les commentaires de toutes les parties prenantes.
4. Établir une feuille de route.
   Sur la base de ces commentaires, déterminer où votre organisme souhaite investir ses efforts.

Notes de fin de texte

[1] Ministère de la Santé (2019, 15 octobre). *Déclaration de valeurs des patients pour l'Ontario*.
[2] Walker, J., Leveille, S. G., Ngo, L., Vodicka, E., Darer, J. D., Dhanireddy, S., ... & Delbanco, T. (2011). *s. Annals of internal medicine Inviting patients to read their doctors' notes: patients and doctors look ahead: patient and physician survey*, *155*(12), 811-819.
[3] Maybee, A., & Greenberg, A. (2019, 7 mars). *.Qualité des services de santé Ontario, Progrès des portails des patients*.
[4] Santé Ontario. (2020a). *Draft Digital Health Information Exchange Policy*.
[5] Kindig, D. A., Panzer, A. M., & Nielsen-Bohlman, L. (Eds.). (2004). *Health literacy: a prescription to end confusion.* National Academies Press.
[6] HIMSS (n.d.). *Interoperability in Healthcare*.
[7]HMT Mag. (2013, 21 février). *Healthcare Innovation Empowering patients through advanced EMR use*.
[8] Health Quality Ontario. (s.d.). *Patient Reported Outcome Measures (PROMs)*.
[9] Kingsley, C., & Patel, S. (2017). *Patient-reported outcome measures and patient-reported experience measures*. Bja Education, 17(4), 137-144.
[10] cyberSanté Ontario. (s.d.). Norme d'authentification unique et de partage des renseignements des patients.
[11] Vreeman, D. J., & Richoz, C. (2015). *Possibilities and implications of using the ICF and other vocabulary ps in electronic health records. Physiotherapy Research International, 20*(4), 210-219.
[12] OntarioMD (n.d. c). *EMR Specifications Library*.
[13] Lehmann, C. U., Petersen, C., Bhatia, H., Berner, E. S., & Goodman, K. W. (2019). *Advance directives and code status information exchange: A consensus proposal for a minimum set of attributes*.
[14]Commissariat à la protection de la vie privée du Canada (2019). *Lois sur la protection des renseignements personnels au Canada*.
[15] Alpert, J. M., Krist, A. H., Aycock, R. A., & Kreps, G. L. (2016). Applying multiple methods to comprehensively evaluate a patient portal's effectiveness to convey information to patients. *Journal of medical Internet research*, *18*(5), e112.

Références

Inforoute Santé du Canada (n.d.*). Accès aux normes*.
Cerner (n.d. a). *DSTU 2 Overview*.
Cerner (n.d. b). *FAQs*.
ClinicalConnect (n.d.). *About ClinicalConnect*.
Epic (n.d.). *Epic on FHIR*.
Ontario. (2019, 1er décembre). *Équipes Santé Ontario : Manuel d'instructions concernant les solutions numériques pour la santé*.
Ontario (2020, 20 avril). *Digital Health Information Exchange Policy*.
Qualité des services de santé Ontario (2020, 12 mars). *Adopting and Integrating Virtual Visits into Care: Draft Clinical Guidance.*